Le droit à la vie privée

De Terwangne, Cécile

Published in:
Quand l'invasion technologique menace nos libertés

Publication date:
2016

Document Version
le PDF de l'éditeur

Le droit à la vie privée : quel sens aujourd'hui ?

Cécile de Terwangne

Introduction

Il s'impose, pour commencer, de baliser le terme clé de cette journée de réflexion : l'expression « droit à la vie privée ». Cette notion est aujourd'hui soumise à d'énormes pressions, ainsi qu'on le verra dans la suite de l'exposé, et suscite le questionnement sur le sens qu'elle peut encore présenter dans la société actuelle, en tant que liberté ou droit fondamental garanti aux individus.

Ce terme de « droit à la vie privée » est reconnu officiellement au niveau européen depuis 1950, année où a été adoptée la Convention européenne des droits de l'Homme. Le droit au respect de la vie privée a en effet été inscrit à l'article 8 de ce catalogue de droits fondamentaux. Or, il est clair que ce que les auteurs de la Convention avaient comme perception de la vie privée en 1950 ne correspond pas à ce qui est entendu de nos jours.

Avant de présenter la nouvelle portée de la notion de vie privée, qui est cruciale aujourd'hui parce qu'il s'agit du dernier rempart contre tous les mouvements et changements qui traversent la société en lames de fond, je voudrais tout d'abord m'attacher à brosser le tableau général de tout ce que les développements techniques présentent comme nouveaux défis et risques pour la vie privée et les droits fondamentaux.

Il est clair qu'on ne peut se cantonner dans la position de celui qui déclare « moi, je n'ai rien à cacher, alors où est le

problème ? ». Face au déploiement des nouvelles technologies, il importe d'être des acteurs éveillés et conscients et non des sujets-objets manipulés, connus, suivis, transparents face aux puissants intervenants publics et privés qui jouent sur la scène ou en coulisses, tirant les ficelles.

C'est à cette démarche de prise de conscience que je voudrais vous inviter aujourd'hui. Une fois le tableau général dressé, tout effrayant qu'il soit, on pourra se pencher sur la réponse apportée par le droit et la protection juridique de la vie privée. Des organismes ont été mis en place, tels la Commission belge de la protection de la vie privée ou la CNIL, l'organe équivalent français (la Commission Nationale Informatique et Libertés). Ces organes ont pour mission essentielle de veiller et de susciter la réflexion pour ne pas tomber dans l'enthousiasme béat devant les « progrès » des TIC, les technologies de l'information et de la communication, pour résister à ce jugement comminatoire : « Vous êtes ringard si vous n'applaudissez pas !»

1. Les risques et défis pour la vie privée et les autres droits

Les points qui suivent sont consacrés aux différents défis et risques que le déploiement des technologies de l'information suscite à l'égard de la vie privée mais également à l'égard d'un ensemble d'autres droits et libertés qui sont aussi en jeu, comme la liberté de mouvement, la liberté d'expression, la liberté d'association ou la liberté de choix de consommation.

1.1 La qualité de l'outil technologique

Avant tout, il faut se rendre compte qu'une des principales sources d'inquiétude et de questionnement vient de la qualité de l'outil technologique.

Dans une série de situations, des données sur un ensemble de personnes étaient déjà récoltées et rassemblées au sein de registres ou de document « papier ». Cela fait en effet des décennies voire des siècles que des données sont, par exemple, recueillies par les pouvoirs publics sur la population dans le cadre de recensements, ou pour élaborer des statistiques, ou encore pour enregistrer les naissances, décès et épisodes de vie des citoyens.

Le changement provient de la puissance des outils technologiques auquel il est désormais recouru pour réaliser les mêmes tâches ou pour atteindre les mêmes objectifs. Cette puissance se traduit en termes de quantité des informations traitées, de variété des opérations réalisables sur ces données, et de vitesse de ces opérations. La quantité de données pouvant être enregistrées sur les supports électroniques actuels est en effet gigantesque et l'on sait, grâce à la loi de Moore, que cette quantité va toujours croissant. A titre d'illustration, il suffit de songer qu'une simple clé USB de type courant (capacité de 32 GB) peut stocker l'équivalent de plusieurs milliers de livres, correspondant à une bibliothèque entière... A cette colossale quantité de données,

il faut ajouter les possibilités d'action offertes par les technologies au sein de ces masses de données, qu'il s'agisse d'enregistrement, de sélection, de corrélation, de suppression de données, etc. Ces opérations ne demandent généralement pas plus de quelques fractions de secondes pour être réalisées, même sur des masses hallucinantes de données. Il est devenu parfaitement simple, aisé et rapide de nos jours de chercher une aiguille dans une botte de foin électronique...

Lorsque les données étaient stockées dans des sources papier, dispersées en différents endroits, la difficulté pratique de consulter ces sources et d'y faire des recherches ainsi que le temps considérable que cela mobilisait, offrait une sorte de protection en soi. Dans l'environnement technologique, où toutes les opérations sont possibles sur cette masse de données et surtout avec une rapidité qui ne décourage personne, l'équilibre trouvé par le passé est remis en cause et des risques d'usages abusifs surgissent.

1.2 Le déploiement des TIC au sein du secteur public

Le développement de l'administration électronique ou de l'e-gouvernement (*e.government)* à partir de l'utilisation des TIC par les administrations publiques a conduit à une organisation en réseau des autorités étatiques. Cette évolution se base essentiellement sur le partage de données entre autorités, sur la création de fichiers de référence et de vastes « entrepôts de données », de même que sur l'interconnexion de bases de données autrefois indépendantes.

On se trouve dès lors en présence d'outils particulièrement performants, soit centralisant une série de données au sein de ce qu'on appelle des « entrepôts de données » (*datawarehouses*), véritables rassemblements de grandes quantités de données, soit mettant en place un réseau thématique, appelé quant à lui « banque carrefour », qui permet d'accéder aux différentes sources de données maintenues séparées mais reliées. Ce dernier modèle est fort

répandu au sein de l'administration électronique belge qui a vu fleurir nombre de « banques carrefour » à la suite de la création de la Banque carrefour de la Sécurité sociale. Cette formule est plus protectrice des individus, dans la mesure où les données ne sont pas rassemblées mais sont maintenues dans leur environnement d'origine. On ne voit pas dès lors l'apparition d'une base de données démesurée qui présente des risques accrus en cas d'intrusion ou d'utilisation non autorisées.

Ce modèle de l'e-gouvernement suscite d'importantes interrogations relatives à la protection de la vie privée. Le modèle antérieur de l'administration « en silos » dans lequel chaque entité disposait d'informations propres, isolées, destinées à réaliser sa mission légale, était présenté comme la garantie contre un État omniscient à l'égard duquel le citoyen serait totalement transparent.

L'« obscurité pratique » était la clé de l'équilibre dans la relation administration-administrés. Cette garantie a disparu au nom de l'efficacité. On doit aujourd'hui impérativement poser la question de la maîtrise par chacun des informations collectées à son propos, de la transparence des échanges et de la proportionnalité des traitements[2].

Par ailleurs, le recours aux identifiants uniques servant d'instruments d'interconnexion et d'accès transversal aux données d'un individu augmente encore les risques de perte de contrôle et de non-respect de la proportionnalité.[3]

Les inquiétudes face aux traitements de données personnelles par les autorités publiques sont accentuées par le fait que ces traitements servent de base à la prise de décisions telles que

[2] Voy. E. DEGRAVE, *L'E-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier, coll. Crids, 2014.
[3] Voy. E. DEGRAVE et C. de TERWANGNE, « Règlement e-IDAS et secteur public : La carte d'identité électronique belge, instrument d'une identité numérique européenne ? », *in L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Larcier, coll. du CRIDS, 2016.

l'octroi d'une pension, la reconnaissance d'un statut particulier, l'établissement de l'impôt, l'ouverture d'enquêtes pénales,...

1.3 Le déploiement des TIC au sein du secteur privé

A. Exploitation de la valeur économique des données

Les données personnelles représentent une valeur économique. Cette valeur est importante à trois niveaux :

- pour les acteurs offrant des services via Internet, car connaître le profil des internautes intéressés par les produits ou services et pouvoir détailler très précisément leur intérêt (pages Web lues, liens cliqués, fréquence des visites...) permettent de configurer l'offre de manière optimale ;
- pour les acteurs exploitant commercialement des bases de données nominatives : récolter des données tous azimuts permet de constituer de très riches bases de données exploitables et revendables pour des activités de ciblage des individus, comme les activités de marketing et de mailing ;
- pour le fonctionnement même du Web : la gratuité de la plupart des services offerts sur le Web n'est que de façade. L'exposition publicitaire des utilisateurs finance l'offre. Le modèle économique repose sur le marketing. Celui-ci sera d'autant plus rentable que le profil des destinataires est précis et permet de cibler efficacement les messages publicitaires. Pour Google et Facebook, par exemple, le profit tiré des activités de marketing opérées sur leurs sites s'élève annuellement à plusieurs milliards de dollars.

Contrairement à ce que l'on pense, la navigation sur Internet laisse bien davantage de traces que déambuler et agir dans la vie réelle. Les actions que l'on effectue sur Internet laissent entre les mains de différentes personnes des traces de ce que l'on a fait (adresse IP, c'est-à-dire l'identification d'un

ordinateur pour le temps d'une session de navigation sur Internet ; fournisseur d'accès ; page Web d'où l'on vient ; historique de la navigation,...). Les outils comme les cookies[4] permettent d'individualiser un ordinateur et, dès lors, son utilisateur. À l'inverse de ce qui se passe dans le monde physique réel, il n'est pas question de se promener sur les inforoutes, d'entrer dans les magasins virtuels, de lire le journal, d'être intéressé par une annonce commerciale,... sans que cela se sache. On ne peut manquer de s'interroger sur cette transparence permanente qui ne serait sans doute pas tolérée dans le monde réel.

Dans les trois schémas ci-dessus, la collecte et le croisement d'informations conduisant à dessiner les profils des utilisateurs deviennent des opérations cruciales. Ces opérations se font toutefois, dans de trop nombreux cas, à l'insu des personnes concernées. Elles impliquent souvent une utilisation des données au-delà des finalités originelles. Et la quantité des données collectées pose inévitablement la question de la proportionnalité. Est-il nécessaire ou tout simplement normal, par exemple, que les moteurs de recherche (comme Google) conservent durant des mois tous les mots introduits par une personne (individualisée et reconnue grâce à un cookie) ? Cet ensemble de mots est le plus souvent incroyablement révélateur des centres d'intérêt, des goûts, des activités, des projets ou même de la santé de la personne qui utilise le moteur de recherche.

Le profilage et le marketing individualisé portent atteinte à la liberté de poser des choix. Nous vivons dans une société où

[4] Le mécanisme des cookies est défini par le protocole de navigation Web (http) et permet à un serveur Web de transmettre au navigateur de l'internaute un petit fichier contenant une série d'informations que celui-ci lui retournera lors des visites ultérieures. Le cookie a une durée de vie limitée, soit liée à la fermeture du navigateur, soit à une date d'expiration qui peut parfois être très lointaine. Les cookies sont donc stockés localement par le navigateur sur le disque dur de l'utilisateur. Les cookies sont utilisés par les serveurs Web à des fins de gestion de session et de personnalisation, mais ils peuvent aussi servir comme un moyen de traçage. De plus, il faut noter que, lors de la visite d'un site, le navigateur peut accéder à des cookies provenant de sites tiers. Cette technique est fréquemment utilisée pour la mesure d'audience ou le profilage publicitaire.

l'on vous connait avant même que vous vous présentiez sur un site Web. A l'instant où vous découvrez un site, celui-ci sait déjà qui vous êtes, quelle langue vous parlez, ce qui vous intéresse,... Les publicités qui vont s'afficher correspondront à des achats ou requêtes effectués sur d'autres pages Web, d'autres sites. Ou l'on vous dira que si vous cherchez à acheter tel produit ou tel livre, vous devriez être intéressé également par tel autre. Si vous avez fait des recherches pour effectuer un voyage dans tel pays, vous verrez apparaitre sur votre écran des publicités ciblées sur ce pays durant les semaines qui suivront.

En conclusion, on vous connait, on prédit vos intérêts et les choix que vous allez poser.

B. Surveillance dans le monde du travail

Les TIC ont mis entre les mains des employeurs des outils de surveillance inimaginables autrefois. Les cartes magnétiques d'accès aux locaux disent à l'opérateur du réseau qui se trouve où et à quelle heure, alors que les clés classiques étaient muettes à ce sujet. Les réseaux de caméras permettent de surveiller les visiteurs aussi bien que le personnel. La surveillance du personnel s'effectue également par le contrôle de la navigation sur Internet et l'usage du courrier électronique mis à la disposition des travailleurs. Pour ceux qui prestent hors des murs de l'entreprise, les systèmes de localisation et de suivi géographique des travailleurs permettent de gérer à distance une flotte de taxis, de dépanneuses ou de camions et de surveiller leurs pérégrinations en temps réel.

Les TIC représentent aussi des instruments de connaissance. Bon nombre d'employeurs se renseignent à la source du Web sur les candidats employés. Google et Facebook, notamment, jouent ainsi le rôle d'indicateurs et révèlent au futur patron des facettes des candidats qui ne se trouvent pas sur leurs CV...

1.4 Outil de localisation mettant à mal la liberté de mouvement

La liberté d'aller et venir, ou liberté de mouvement, est insidieusement mise à mal dans un monde où tous nos déplacements sont traqués.

Les mouchards sont les cartes de métro ou de transports en commun qui sont passées du vieux support cartonné à la puce électronique indiquant le lieu, le jour et l'heure du passage à la borne. Ces informations, couplées à l'identité du détenteur de la carte dès qu'il s'agit d'un abonnement, sont accumulées entre les mains des responsables du système et peuvent être partagées ou vendues à d'autres intervenants.

Les téléphones portables sont aussi des espions embarqués dans les poches de nos vestes et pantalons. Ils nous géo-localisent, même par défaut dans les dernières versions des smartphones les plus en vue. Ils comptent nos pas et calculent le dénivelé de nos trajectoires, pour surveiller la quantité d'énergie brûlée et nous édifier sur les risques de vies trop sédentaires.

Les puces RFID collées sur les étiquettes des vêtements et sur les objets[5], les GPS intégrés dans les appareils photos, les

[5] « La technologie RFID (*Radio-Frequency IDentification*) est une technique d'identification qui se base sur trois composants : l'étiquette, ou tag, qui est collée ou intégrée à l'entité à identifier ; le lecteur, utilisé pour interroger le tag lorsque celui-ci est à sa portée ; le système d'information, qui reçoit l'information du lecteur et la traite.
Le tag est composé d'une antenne et d'une puce électronique, qui contient, au minimum, un identifiant. Lorsque le tag est interrogé par un lecteur (par l'utilisation d'ondes magnétiques), il transmet son identifiant au lecteur. La structure du tag est très simple, de manière à permettre une production de masse à un coût autorisant son utilisation massive, typiquement quelques centimes. La lecture du tag ne nécessite pas de contact entre celui-ci et le lecteur ; en fonction du type de tag, la distance de lecture peut varier entre quelques centimètres ou quelques dizaines de centimètres, voire au-delà.
Les tags RFID sont utilisés dans la gestion des stocks et de l'approvisionnement, pour les péages routiers, dans la grande distribution pour la gestion de l'inventaire, des caisses ou du service après-vente, dans les aéroports pour le suivi des bagages ou comme moyen de marquage des animaux. Dans certains cas, les tags peuvent être implantés chez des êtres humains, par exemple pour assurer la sécurité d'enfants ou de personnes

clés électroniques des portes des bureaux (cf. *supra,* point 1.3.B.) ou des chambres d'hôtel, sans même parler des caméras de vidéo-surveillance qui ont fleuri à tous les coins des rues, parkings, banques, gares, etc., tissent la trame d'une société dans laquelle il est désormais difficile d'errer incognito...

Nous vivons donc dans une « société de traçage ». On surveille les déplacements sous toutes leurs formes. Et le « on » peut être tant un acteur du secteur privé, l'entreprise qui utilise les bornes, celle qui vend les abonnements de smartphones ou celle qui offre des applications à intégrer dans ceux-ci, qu'un acteur du secteur public, police, agence de renseignement ou autre.

1.5 Outil de diffusion

Les nouvelles technologies sont aussi un formidable outil de diffusion des données et des informations. Bien sûr, il y a Internet avec ses sites web, ses blogs, ses forums, ses réseaux sociaux, ses sites de vidéos, de partage de photos, de discussions,...

Si l'on se place du point de vue de l'émetteur, on observe qu'il a désormais à sa disposition un attirail de solutions pour faire passer son message au public visé, que ce public soit sélectionné et restreint, ou qu'il corresponde potentiellement au monde entier. La liberté d'expression, en ce sens, est exacerbée par les technologies de l'information et de la communication.

Si l'on se place par contre du côté de la personne objet d'un message, d'une photo, d'une vidéo, on découvre le pouvoir exercé par autrui sur son « image informationnelle », c'est-à-dire tant sur son image proprement dite que sur les

âgées, ou, dans un registre plus léger, pour surveiller l'accès ou gérer les consommations dans une discothèque. » (J.-N. COLIN, C.de TERWANGNE, « Protection de la vie privée et des données personnelles dans l'environnement numérique », in C. de Terwangne (ed.), *Vie privée et données à caractère personnel,* Bruxelles, Politeia, 2013, ch. 1.2., pp. 5-6).

informations qui se rapportent à cette personne. Loin de maitriser cette image informationnelle, on découvre le pouvoir que d'autres peuvent exercer du fait qu'ils détiennent des informations ou tout simplement qu'ils tiennent en main un téléphone portable (*smart phone*) avec appareil photo et caméra intégrés.

Les individus peuvent désormais être très facilement à l'origine d'intrusions dans la vie privée d'autres individus. Lorsqu'ils font usage du réseau et de toute la variété de services en ligne existant, que ce soit par le biais d'un ordinateur, d'un téléphone portable ou d'une tablette, ils ne savent pas ce qui sera fait en aval de leur activité de communication d'images et d'informations, ils ne peuvent contrôler à distance tout ce qui sera fait de ce qu'ils diffusent. Dans bien des cas, ils ne prennent pas la pleine mesure de la portée de leurs actions sur le réseau. Le Web 2.0 leur a donné la possibilité d'interagir, d'apporter des commentaires, de diffuser du contenu, de partager en continu savoirs, photos, vidéos, informations, états d'âme... Toutefois, le rayonnement de l'information sur Internet dépasse parfois largement ce à quoi on s'attend. L'exemple des informations tirées des pages publiques de Facebook et jointes automatiquement, à l'insu de la personne concernée, par un logiciel de courrier électronique, aux courriels envoyés est un premier exemple. La puissance des robots « ratisseurs » qui alimentent les moteurs de recherche permet de faire remonter des informations trouvées à des endroits épars, publiées dans des contextes qu'on croyait particuliers à des personnes qu'on croyait restreintes. Ce qui est émis dans un certain cercle (p. ex., un commentaire déposé sur un forum de discussion) risque donc de réapparaître, sorti de son contexte et juxtaposé à d'autres informations.

Une fois l'information (texte, image, vidéo) diffusée, on ne peut plus contrôler son parcours. L'effacer du site initial n'empêchera pas qu'elle perdure dans les lieux où elle a été copiée ou téléchargée avant son effacement. Et il est illusoire de vouloir contrôler que l'usage qui est fait de l'information

(notamment aux antipodes et par des inconnus) respecte la finalité de sa diffusion première.

Cette perte de contrôle est d'autant plus inquiétante qu'elle s'accompagne de l'*eternity effect*. À l'inverse de la mémoire humaine, la mémoire électronique n'efface rien si ce n'est volontaire. Au niveau technique, il faut en effet faire un effort pour effacer. Effacer est coûteux. Il faut payer quelqu'un qui prenne le temps de sélectionner et procède à l'effacement. Tant qu'on n'a pas pris la décision, le temps et l'énergie de les supprimer (là où on a la maîtrise de la suppression), des éléments peuvent remonter éternellement du passé. Le passé devient « omni-présent ».

Des actes individuels malveillants peuvent aussi susciter des inquiétudes. Diffuser une information diffamatoire ou confidentielle sur Facebook, poster une vidéo intime ou humiliante sur YouTube, ou créer un faux article sur quelqu'un dans Wikipédia peut causer des dommages d'une ampleur sans précédent dans la vie *off line*.

1.6 Outil de transfert

Les TIC sont aussi un outil de transfert. Il n'y a plus véritablement de frontières ni de fuseaux horaires dès qu'on fonctionne avec Internet. Les données ne sont plus facilement localisables, d'autant plus quand elles sont stockées dans le *cloud*. Elles circulent et sont échangées en toute facilité. C'est le règne de ce qu'on appelle les flux transfrontières de données.

Les législations protectrices doivent donc tenir compte de ce phénomène, sous peine de ne plus protéger que les situations situées à l'intérieur des frontières de l'Etat qui les a adoptées, ce qui ne représenterait qu'une parcelle des situations méritant protection. Un régime juridique doit donc être élaboré pour accompagner les flux de données vers des Etats tiers.

Des flux spécifiques de données personnelles sont également apparus, tels les échanges de données sur les passagers aériens. A la suite des attentats du 11 septembre 2001, les Etats-Unis ont mis en place un *Passenger Name Record*, c'est-à-dire un fichier contenant toute une série de données (identifiant, carte de crédit, voyage professionnel ou non,...) sur les passagers aériens provenant de différents continents ou pays, à destination des Etats-Unis. Par la suite, d'autres pays ont emboité le pas aux Etats-Unis sur cette voie et bientôt l'Union européenne va se doter elle aussi d'un tel outil de lutte contre le terrorisme.

1.7 Outil de surveillance

La surveillance technique est omniprésente, via les caméras tout d'abord, que ce soit dans les rues et les parcs, au travail, dans les aéroports et les gares, dans les magasins, dans les entrées d'immeubles, dans les écoles, et jusque dans les maisons grâce aux paquets-cadeaux permettant l'installation de circuits de caméras privés que l'on peut s'offrir à Noël...

Même les parents angoissés qui veulent absolument savoir en permanence où leur enfant ou leur adolescent se trouve peuvent suivre celui-ci à la trace, que ce soit à travers les caméras installées à la crèche et connectées à Internet, ou à travers le suivi des téléphones géolocalisés des jeunes (cf. *supra*, point 1.4. Outil de localisation). Or, dans ce cas, au problème au regard de la liberté et du droit à la vie privée de l'individu même mineur, s'ajoute un problème d'ordre psychologique, sur le plan du développement de l'autonomie de l'enfant.

Par ailleurs, les données liées à l'utilisation d'Internet et des nouveaux moyens de communication représentent une mine de renseignements précieux pour les activités de recherche policière et de lutte contre la criminalité.

Depuis les attentats du 11 septembre 2001 (encore eux...), des textes ont été votés au niveau européen pour harmoniser

les situations dans lesquelles des données relatives au contenu des communications électroniques ou des données de trafic ou de localisation sont conservées pour être tenues à la disposition des autorités pénales. Ces données portent sur la durée, la date, les destinataires, le lieu de toutes les communications échangées, le volume des SMS/textos et des courriels... La directive 2006/24 du 15 mars 2006 sur la conservation de données, imposait ainsi aux fournisseurs de services de communication (Internet, téléphones, mobiles, fax) la rétention des données de trafic et de localisation de tout le monde, de façon systématique et pour une durée variant entre six mois et deux ans...

L'admissibilité d'une telle obligation de conservation systématique et indiscriminée des données liées aux communications via la téléphonie fixe, mobile, par Internet ou via le courrier électronique, de même que les données liées à la navigation sur Internet, a été contestée dans un grand nombre d'Etats membres de l'Union européenne. Au final, cette directive a été déclarée invalide par la Cour de Justice de l'Union européenne 8 ans après avoir été adoptée mais les lois nationales qui avaient été votées dans l'intervalle pour transposer cette directive sont restées en place dans de nombreux Etats membres. La Belgique, quant à elle, a annulé la loi prise en la matière, estimant que cette loi présentait les mêmes défauts que la directive et devait donc subir le même sort[6]. Une nouvelle loi est donc en préparation.

Enfin, il convient de relever que la liberté d'expression et la liberté d'association sont menacées dans une société de surveillance parce que, à partir du moment où ils se sentent surveillés, les individus n'osent plus s'exprimer librement ni fréquenter des groupes ou des personnes de leur choix, dès lors qu'ils ne savent pas quelles en seront les conséquences,

[6] Voy. C. de TERWANGNE, « Il y a des limites à la conservation des données dites 'de connexion', ou quand la Cour constitutionnelle et la Cour de justice de l'Union européenne se donnent la main pour protéger la vie privée », Justice-en-ligne, 28 septembre 2015, http://www.justice-en-ligne.be/article747.html

entre les mains de qui ou de quelles autorités ces informations pourront tomber, ni ce qui sera fait de ces informations.

1.8 Outil de profilage

Le profilage consiste à appliquer des algorithmes à des quantités d'informations agrégées, pour mettre au jour des corrélations entre les données et faire surgir des profils. Ces derniers sont appliqués à un individu, pour décider du traitement à lui réserver (le considérer ou non comme fraudeur fiscal ou comme cible de marketing de tel produit ou comme voyageur candidat terroriste...). Motivé par un intérêt économique (*cf.*, *supra*, point 1.3.), sécuritaire (*cf.* point 1.7.) ou autre, le profilage est facilement réalisable à partir des informations disponibles à grande échelle (traces, mots introduits dans les moteurs de recherche, etc.) et du recours aux cookies, notamment.

Le profilage répond à des besoins ou intérêts légitimes de la société : analyse du risque, identification des fraudes, segmentation des marchés, ajustement de l'offre à la demande, etc. Toutefois, il peut amener à priver des individus de manière injustifiée de l'accès à certains services. L'existence de profils conduit à ce que l'information offerte est filtrée, triée, sélectionnée en fonction du destinataire. Cela vaut aujourd'hui massivement pour les informations commerciales. Sera-ce demain le cas pour toute information ? Le profilage risque aussi d'être un instrument de discrimination. Comment contester l'élaboration d'un profil ou son application inappropriée ? La plupart du temps, l'existence des profils échappe à la connaissance des individus concernés et la compréhension de leurs critères d'élaboration échappe à ceux qui les appliquent. Enfin, l'activité de profilage suscite de graves préoccupations concernant la proportionnalité. Les quantités de données collectées et la durée de leur conservation sont, dans bien des cas, totalement excessives.

2. Notion de vie privée et protection juridique

2.1 Notion de vie privée revisitée

La vie privée, dans le contexte qui nous occupe, ne doit pas se comprendre de façon traditionnelle comme une sphère intime à protéger, contenant un ensemble d'informations privées, voire confidentielles, que l'on souhaite garder cachées. Cette vision est correcte mais trop réductrice de la notion couverte par ces termes.

La vie privée doit se comprendre comme la faculté d'autodétermination, d'autonomie, la capacité de l'individu d'effectuer des choix liés aux informations qui le concernent. La « vie privée » dans ce contexte, c'est la maitrise des informations qui se rapportent à soi. En la matière, il s'agit donc du droit pour l'individu de « savoir ce qui se sait sur lui », de connaître les données qui sont détenues à son propos, par qui, d'en maîtriser les circuits de communication, d'en contrecarrer les utilisations abusives.

La vie privée ne se réduit donc pas à une quête de confidentialité ou d'intimité, c'est la maîtrise par chacun de son image informationnelle ou des données à caractère personnel le concernant.

2.2 Loi relative à la protection des données à caractère personnel

Depuis 1992, une loi assure, en Belgique, la protection des individus face à l'utilisation de leurs données à caractère personnel ; il s'agit de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Cette loi instaure un devoir de transparence concernant l'utilisation des données personnelles : il faut prévenir les

personnes quand on traite des informations sur elles, on doit leur annoncer qui l'on est et pourquoi on traite ces informations. La loi fixe aussi les règles d'utilisation des données personnelles : ce que l'on peut et ce que l'on doit faire avec les données recueillies. La loi instaure également de nouveaux droits pour les personnes fichées dans des registres ou des banques de données : droit d'accès aux données enregistrées, droit de rectification, droit d'opposition, droit de recours.

Le 24 octobre 1995, une directive européenne a été adoptée pour harmoniser les règles de protection des données personnelles sur tout le territoire de l'Union européenne. Comme tous les autres États membres, la Belgique devait transposer dans son droit interne les principes contenus dans la directive. La loi du 8 décembre 1992 a en conséquence été fortement modifiée par la loi du 11 décembre 1998.

Il n'est pas le lieu ici de présenter cette législation de protection de la vie privée et des données dans tous ses détails. On se focalisera sur les éléments de cette loi qui répondent en particulier au problème d'opacité et de déficit de transparence relevé au point 1. ci-dessus, ainsi que sur les droits dont sont désormais armés les individus en réponse au souci de rééquilibrer les rapports entre les personnes qui voient leurs données traitées de toutes parts et les personnes qui tirent un intérêt ou un bénéfice de ces activités de traitement des données.

A. Principe de loyauté

Un des principes essentiels du régime de protection mis en place par la loi, c'est le principe de transparence. L'idée est de faire régner la transparence au sein des utilisations de données personnelles, de lutter contre l'opacité. Pour maitriser ses données, la personne doit en effet savoir ce qui se passe, ce qui est fait avec celles-ci, le sort qui leur est réservé.

Dans la ligne de ce principe de transparence, la loi exige que la collecte des données personnelles soit loyale (article 4, §

1er, al. 1erde la loi). Cela signifie que celui qui a l'intention de récolter des données afin de les traiter doit agir de manière transparente : il doit se faire connaitre et indiquer pourquoi il veut obtenir des données personnelles. Il ne peut faire croire qu'il poursuit un but alors qu'il a l'intention de faire autre chose avec les informations recueillies. Il ne peut pas non plus agir à l'insu des personnes (p. ex., en plaçant des caméras vidéo ou en filmant avec son GSM une personne dans un lieu privé sans la prévenir qu'elle est filmée).

La loi (article 9) impose de fournir des informations aux personnes auprès desquelles on recueille des données, à moins que ces personnes soient déjà informées. Outre ce qui vient d'être dit sur l'indication des objectifs de la collecte, il faut signaler :

- le nom et l'adresse du responsable du traitement et, éventuellement, de son représentant en Belgique ;
- les destinataires ou les catégories de destinataires des données (personnes à qui les données seront communiquées) ;
- le caractère obligatoire ou non de la réponse, ainsi que les conséquences éventuelles d'un défaut de réponse ;
- l'existence pour chacun d'un droit d'accès aux données qui le concernent et d'un droit de rectification de celles-ci ;
- si les données seront traitées à des fins de marketing direct (démarches publicitaires) ; il faut signaler aux personnes concernées qu'elles disposent du droit de s'opposer gratuitement à un tel traitement.

Celui qui ne fournit pas ces informations lorsqu'il collecte des données s'expose à une amende.

B. Droits octroyés au sujet des données

Le législateur a été attentif à essayer de rétablir l'équilibre entre les acteurs en garantissant des droits à toute personne qui voit ses données traitées par autrui. Ainsi, toute personne, quels que soient son âge, son domicile ou sa nationalité, se voit reconnaître les droits suivants vis-à-vis des personnes qui traitent des données sur elle.

Le droit à la curiosité (article 10, § 1er, a, de la loi)

Chacun a le droit d'interroger tout responsable de traitement pour savoir s'il détient ou non des données sur lui. Le responsable interrogé doit confirmer ou non s'il détient des données le concernant et, si c'est le cas, il doit préciser dans quel but il détient les données, de quelles catégories de données il s'agit et quels sont les destinataires de ces données.

Le droit d'accès direct (article 10, § 1er, b, de la loi)

Chacun a le droit de recevoir, sous une forme intelligible, une copie des données faisant l'objet d'un traitement, ainsi que toute information disponible sur l'origine des données. Le droit de connaître la provenance des données utilisées est particulièrement important, car c'est souvent la question de la source des informations qui préoccupe les personnes concernées. Il est important de pouvoir contrôler si la source avait bien le droit de communiquer les données en question. Si des données erronées circulent, il est aussi bien plus efficace de faire corriger à la source les erreurs afin d'arrêter les flux néfastes.

Il arrive qu'une décision affectant de manière significative une personne soit prise sur le seul fondement d'un traitement automatisé (p. ex., cela peut être le cas pour l'octroi d'un prêt ou la souscription d'une assurance). Dans ce cas, la personne en cause doit avoir aussi accès, si elle le souhaite, à la logique qui sous-tend le traitement automatisé en question, c'est-à-

dire au raisonnement automatisé qui a été appliqué pour conclure à la décision (article 10, § 1er, c, de la loi).

Le droit d'accès indirect

En deux circonstances, c'est un accès indirect de la personne concernée à ses données qui est prévu.

L'accès aux *données relatives à sa santé* peut s'effectuer soit directement par la personne sur qui portent les données, soit par l'intermédiaire d'un professionnel des soins de santé choisi par cette personne, si le responsable du traitement ou la personne elle-même demande l'intervention d'un intermédiaire (article 10, § 2, de la loi).

Pour les *données traitées à des fins de sûreté de l'État, de sécurité publique, de défense nationale, de prévention ou de répression des infractions*, c'est également un accès indirect qui est mis en place (article 13 de la loi). Dans ces cas, il faut s'adresser à la Commission de la protection de la vie privée en apportant la preuve de son identité et en lui demandant d'effectuer la démarche d'accès. La Commission effectue les vérifications utiles, fait procéder aux modifications nécessaires et spécifie à l'intéressé qu'il a été procédé aux vérifications, sans pouvoir pour autant en révéler la teneur.

Le droit de rectification (article 12, § 1er, de la loi)

Chacun peut, sans frais, faire rectifier les données inexactes qui se rapportent à lui et faire effacer ou interdire d'utilisation les données incomplètes, non pertinentes ou illégales.

Le responsable du traitement doit répondre dans le mois à celui qui a demandé les corrections. Il doit indiquer les rectifications ou effacements qu'il a effectués. S'il ne le fait pas, on peut s'adresser à la Commission de la protection de la vie privée en dénonçant son comportement. On peut également porter plainte en justice.

En outre, si des données inexactes, incomplètes, non pertinentes ou interdites ont été transmises à des tiers, le responsable doit, dans le mois, signaler les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées, à moins que cela ne s'avère impossible ou extrêmement difficile.

Le droit d'opposition (article 12, § 1er, al. 2 et 3, de la loi)

Chacun a le droit de s'opposer à ce que les données le concernant fassent l'objet d'un traitement, mais il doit invoquer des raisons sérieuses et légitimes. Ce droit d'opposition n'est toutefois pas admis pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat ni pour les traitements de données imposés par une obligation légale.

Lorsque les données sont collectées *à des fins de marketing direct* (pour des démarches publicitaires), la personne concernée peut s'opposer gratuitement et sans aucune justification au traitement de ses données. Ainsi, lorsque l'on est invité à remplir un talon-réponse, si celui qui récolte les données a l'intention de les transmettre à des sociétés de marketing direct, il doit le mentionner sur le talon et on a le droit de s'opposer sans justification à ces transmissions. De même, celui qui est importuné par des propositions téléphoniques pour découvrir des salons de cuir ou déguster des vins peut exiger d'être radié de la liste de celui qui téléphone.

Le droit de ne pas être soumis à une décision automatisée (article 12bis de la loi)

Il n'est pas souhaitable qu'une décision qui s'impose à un homme dépende des seules conclusions d'une machine. Aussi, la loi interdit qu'une décision affectant une personne de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.

Toutefois, cette interdiction ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat (p. ex., pour l'octroi d'un prêt ou la souscription d'une assurance) ou est fondée sur une disposition légale ou réglementaire. Le contrat ou la disposition en question doivent contenir des mesures garantissant la sauvegarde des intérêts de l'intéressé. À tout le moins, celui-ci doit avoir le droit de faire valoir *utilement* son point de vue.

Le droit de recours (article 31 de la loi)

Il convient encore de préciser que la loi Vie privée a veillé à offrir aux personnes qui auraient des difficultés à exercer ou à faire respecter l'un des droits présentés ci-dessus une voie de recours simple, rapide et gratuite. Il s'agit d'un recours auprès de la Commission de la protection de la vie privée.

Ainsi, la personne concernée peut adresser une plainte à la Commission de la protection de la vie privée. Cette Commission interviendra pour amener le responsable du traitement à respecter les obligations que lui impose la loi. Elle s'efforce généralement de résoudre les litiges à l'amiable. En cas d'insuccès, la Commission émet un avis sur le caractère fondé de la plainte. Si elle constate une infraction, elle la dénonce au procureur du Roi.

La personne concernée peut aussi choisir de porter le litige directement devant un tribunal.

Conclusion

Au terme de cette contribution, on ne peut que conclure en insistant sur l'importance d'avoir les yeux ouverts sur le sort qui est réservé aux données personnelles dans la société d'information et de surveillance dans laquelle on vit aujourd'hui. Il est par ailleurs crucial d'avoir conscience de la valeur économique de ces données et dès lors de la convoitise dont elles sont l'objet. Enfin, il importe de savoir que des réponses juridiques ont été mises en place face aux défis et aux risques nés des développements technologiques pour la vie privée et pour les autres droits fondamentaux.